H-5

JOURNAL of ELECTRONIC DEFENSE • OCT '84

Protective C^3CM

An OPSEC Objective

WALTER G. DEELEY
Deputy Director Communications Security
National Security Agency

Protective C^3CM attempts to prevent an adversary from destroying our critical C^3 facilities and to protect our communications against jamming and intrusion. The National Security Agency (NSA), has a vital interest in this area. It is responsible for US communications security (COMSEC) including secure communications practices and procedures, and advising on the selection and use of COMSEC equipment and systems. It also vigorously fosters effective control of emissions. These measures reduce an adversary's capability to identify and target our C^3.

A Protective C^3CM program must effectively identify COMSEC and other security vulnerabilities, and recommend corrective measures. Over the years, in supporting a wide variety of military and other government operations, NSA has found the Operations Security (OPSEC) process to be the most effective method of accomplishing this objective.*

In OPSEC, operational considerations, intelligence analysis techniques, and a variety of security disciplines are brought to bear on specific problems.

OPSEC's goal is to enhance operational effectiveness by protecting that information which an adversary *must* have in order to counter our operations. Early OPSEC surveys tried to identify and eliminate sources of exploitable information pertaining to our imminent military operations. This objective still figures prominently in OPSEC, but our experience indicates that the OPSEC process can be applied to virtually any government operation, program, or function which could be exploited by an enemy.

For example, an adversary might try to prevent us from effectively using our close air support aircraft, or from executing our retaliatory nuclear forces. Countering these objectives by identifying and protecting the information needed to accomplish this, is typical of the type of problem effectively addressed by OPSEC.

Every OPSEC study begins with the development of Blue (friendly) and Red (enemy) force data bases. The collected data is analyzed to identify Blue force's susceptibility to intelligence exploitation and to determine the Red force's ability to detect and exploit them. The results are then analyzed to estimate the relative significance of each type and source of information that the enemy could intercept and use to his advantage.

The Blue force data base is developed by interviewing the people who support and carry out an operation or function. As a rule, it is not profitable to rely on adversarial exercises to gather information. Empirical studies, such as those conducted by COMSEC monitors, may well be essential to obtaining signal or propagation characteristics, resolving conflicting allegations, or illustrating a security weakness, but the need for such studies should follow from the initial analysis. Reliance on adversarial attacks for data base development is needlessly time consuming, expensive, and often leads to erroneous conclusions. The information collected is often fragmentary, and seldom affords insight into the underlying causes of security weakness. In short, we simply cannot spend the time and money that an adtrol of the executing force, there may be other peripheral activity, such as radar tracking, which could be observed by an enemy.

The susceptibility of each event to exploitation must be determined, a process which requires the expertise of skilled analysts in each of the pertinent intelligence or security disciplines. Empirical studies can be arranged at this point to address specific questionable issues, but it will be found that communications-electronics susceptibilities, for the most part, are readily apparent to COMSEC analysts. Plain-language communications would be evaluated from the standpoint of their explicit intelligence value, as well as their inferential value in relation to other communications and observable events. Communications practices and procedures, such as frequency and callsign usage, would be examined for weaknesses which an adversary could exploit to identify specific organizations for targeting or to predict forthcoming activity. Since most types of US military activity are often characterized by distinctive patterns in the timing, volume, and directional flow of their communications, analysts would seek to isolate patterns and determine their significance. Signal characteristics would also be addressed to determine if there are susceptibilities to radiofingerprinting and position locating techniques.

After completing this process, each event in the Blue force sequence that is judged susceptible to intelligence exploitation is arrayed against known or estimated Red force capabilities. The products of this comparison of susceptibilities and adversary threat capability are statements of vulnerabilities.

It is not uncommon to find that a multitude of vulnerabilities have been identified. While it is almost axiomatic that an adversary can acquire some information of intelligence value, the critical issue is whether or not he will acquire the information he needs to achieve his objectives.

Because of the complexity of this type of problem, NSA has advocated using operations analysis techniques in all OPSEC assessments to help determine the relative significance of specific vulnerabilities. One such technique, a variation on a commonly accepted decision analysis routine, has proved especially useful.

A key feature of the assessment process is refinement of the OPSEC objective. "The identification and protection of information which an adversary must have to keep us from using our Close Air Support assets effectively," is typical of many general OPSEC objectives. However, the scope of a problem stated in such terms could require consideration of a sizeable number of adversary scenarios aimed at countering CAS operations.

By examining the event-sequence list and vulnerability information developed by the survey portion of the OPSEC study, analysts and command operations personnel are able to identify events which are critically important to a successful mission. The purpose is to see if an adversary could exploit specific vulnerabilities to keep those critical events from being accomplished and also to identify the most likely ways he might attain his objective.

In the case of CAS operations, we can focus on those specific vulnerabilities which enable an adversary to destroy critical C^3 facilities, jam critical communi-

Continued

*The National Security Agency developed the data collection and analysis techniques that were used in the first OPSEC study and were subsequently embodied in OPSEC methodology. These techniques have proven to be the most successful means of identifying, assessing, and eliminating security weaknesses.

cations links, or intrude on communications systems.

Operations security analysts, working closely with command operations and intelligence personnel, postulate adversary strategies — sequential steps of what the adversary must know and do to carry out his attacks successfully. The options available to the adversary for accomplishing each step are defined and probabilities assigned to indicate the likelihood of completing a step successfully.

In the somewhat simplistic example shown in table 2, it is considered that the enemy will attempt to undermine CAS operations by jamming the critical communications link between the Forward Air Control Party (FACP) and the CAS aircraft. For the purposes of illustration, it is stipulated that the callsigns and frequencies used in planning and executing the CAS mission are unchanged from thosed used in peacetime exercises; further, that the circuit used to request CAS support is unsecured.

Given the stipulations of the strategy depicted in table 2, the overall probability of the enemy successfully jamming the CAS/FACP communications link on detection is calculated to be 83 percent; the probability of successfully detecting and following frequency changes is 62 percent. We consider these figures to be "soft," i.e., they are rough estimates of high possibilities of enemy success rather than assertions of precise probability. The estimates are nevertheless a valid guide and are of considerable value in demonstrating the benefits of any security measures proposed to counter the enemy strategy.

Security measures are selected to keep the enemy from completing one or more steps in his attack strategy. If, for example, we could keep the enemy from knowing that CAS support had been requested for a geographical area or from knowing that the CAS/FACP communications link was critical to successful air support, he might well direct his intercept and jamming assets to other, seemingly more lucrative targets.

For the purpose of illustration, however, let us say that OPSEC analysts in collaboration with command operations and communications personnel decide to attack step 3 in the adversary's strategy.

If changing callsign and frequency systems were used in all *peacetime* CAS exercises and operations, the rapid acquisition and recognition of CAS/FACP communications would be severely inhibited. The probability of the adversary knowing the frequency used on the CAS/FACP link as a result of intercepting the communications of previous exercises is nil. Further, the probability of an enemy agent being able to acquire and pass the frequency for a single forthcoming operation would be very low.

TABLE I

EVENT	TIME
Ground force requests the Tactical Air Control Center (TACC) to provide CAS.	TOT — 24 Hrs.
TACC/ATOC sends Air Tasking Order to Wing Operations Center (WOC).	TOT — 22 Hrs.
WOC sends Operations Order to the CAS squadron and to the commands that will provide Electronic Warfare (EW) and Air Refueling (AR) support to the CAS aircraft.	TOT — 15 Hrs.
CAS aircraft preparation	TOT — 8 Hrs.
Tanker takeoff	TOT — 3 Hrs.
EW aircraft takeoff	TOT — 1.5 Hrs.
CAS aircraft takeoff	TOT — 1.2 Hrs.
Tanker aircraft reach AR track	TOT — 1.10 Hrs.
CAS aircraft start refueling	TOT — 50 Min.
CAS aircraft end refueling	TOT — 30 Min.
EW aircraft on station	TOT — 20 Min.
CAS aircraft, on station In Area of Operations (AO), contacts the Forward Air Control Party (FACP)	TOT

TABLE II

Enemy Objective: Stop/Inhibit CAS by jamming FACP communications.

Step 1: Know CAS support requested	
Option 1: Intercept request for support	.90
Option 2: Agent report	.05
Option 3: RECCE detects CAS preparation	.50
Step 2: Know CAS/FACP radio link critical	
Option 1: Open source Information	.90
Option 2: Intercept of peacetime exercises	.90
Option 3: Agent reports	.75
Step 3: Know freqs. used on CAS/FACP link	
Option 1: Intercept of peacetime exercises	.90
Option 2: Agent reports	.25
Step 4: Jam CAS/FACP link on detection	.95
Step 5: Detect and follow freq. changes w/jammer	.75

Looking again at table 2, if we accordingly set the probability of Option 1 of Step 3 at 0, and the probability of Option 2 at .05, our new computation of the overall probability of the enemy successfully jamming the CAS/FACP communications would be less than 5 percent!

Using the same method, we could calculate the impact of using other approaches, such as low probability of intercept or anti-jam equipment. Each could give a different measure of effectiveness.

CONCLUSION

At NSA, we recognize that there are pitfalls inherent in the subjectivity of the assessment process described above. The process is only as good as the analysts working the problem and the validity of the data available to them. We are working, however, to develop more effective means of quantifying the benefits of security to military commanders. Such measurements are often a critical consideration in ensuring that COMSEC is effectively and economically applied.

We are convinced that it is not necessary to provide uniformly high security to all communications. We know from past experience that substantial gains in security can often be achieved cheaply by procedural changes which impact only slightly on operational efficiency. The problem, however, is to identify the precise security needs for commanders.

In the case of protective C^3CM, we want to conceal or otherwise protect our critically important communications links and nodes. We can make some of these communications more difficult for an adversary to acquire, we can hide them amid the mass of unimportant electromagnetic activity, and we can build systems which can work through various types of jamming. Critical nodes, our command, control, and communications facilities can be concealed by remoting of antennas, judicious routking of communications, and procedures designed to confuse or mislead an adversary. The means of protection must always answer the threat — the probability that an adversary can achieve his offensive C^3CM objectives against us.

We believe that the OPSEC process is an ideal method for determining security needs with some precision. NSA, in collaboration with the Service Cryptologic Elements, stands ready to support military commanders in using OPSEC to identify, analyze, and assess their protective C^3CM problems.

Walter G. Deeley, *has been the Deputy Director for Communications Security, National Security Agency, since June 1983. He has served with NSA and its predecessor organizations since 1948.* ■